SAVONIA

Tekniikka

Palopäällystön koulutus

OPINNÄYTETYÖ

SOPIMUSPALOKUNTIEN TIETOTURVA JA TIETOSUOJA OULU-KOILLISMAAN PELASTUSLIIKELAITOKSELLA

Marko Heikkilä

23.11.2015

SAVONIA–AMMATTIKORKEAKOULU - TEKNIIKKA, KUOPIO

Koulutusohjelma

Palopäällystön koulutusohjelma

Tekijä

Marko Heikkilä

Työn nimi

Sopimuspalokuntien tietoturva ja tietosuoja Oulu-Koillismaan pelastusliikelaitoksella

Työn laji	Päiväys	Sivumäärä
Opinnäytetyö	9.11.2015	37+6

Työn valvoja	Yrityksen yhdyshenkilö
yliopettaja Mari Lyyra	

Yritys

Tiivistelmä

Tämän opinnäytetyön tarkoituksena on selvittää, miten tietoturva ja tietosuoja on järjestetty Oulu-Koillismaan pelastuslaitoksen sopimuspalokuntalasille sekä sivutoimiselle henkilöstölle sekä miten koulutus on huomioitu harjoitusohjelmissa.

Tietoturva ja tietosuoja ovat aiheena laajoja, joten kysymysten asetteluissa, jotka koskevat sopimuspalokuntatoimintaa, joutuu rajamaan tarkkaan ne kysymykset, joilla on asiaan merkitystä. Kysymykset lähetettiin Webropol-kyselyinä kaikille pelastuslaitoksen alueen sopimuspalokunnille sekä sivutoimisille palomiesyhdityksille. Lisäksi kysely osoitettiin alueen vakinaiselle henkilöstölle, jotka toimivat alueella sopimuspalokuntien kouluttajina ja harjoitusohjelmien hyväksyjinä. Kyselyjen lisäksi tehtiin haastatteluja.

Sopimuspalokuntalaisten rooli hälytystehtävistä pelastuslaitoksen alueella on merkittävä. Alueella toimii vakinainen miehistö ympäri vuorokauden Kuusamossa, Oulussa, Haukiputaalla ja Kempeleessä.

Tietoturvan ja tietosuojan kannalta tärkeää on se, että tehtävistä, mitä sopimuspalokuntalaiset tekevät eniten, ovat ensivastetehtävät ja liikenneonnettomuudet, joissa liikkuu eniten tietoa ihmisistä. Tämän vuoksi, on tärkeää, että tietoturva ja tietosuojakoulutusta järjestetään. Tässä työssä tuli esille, että koulutusta ei ole järjestetty riittävästi ja asia pitäisi huomioida paremmin harjoitusohjelmia laadittaessa. Asian esille nostaminen sai vastaajilta kiitosta.

Avainsanat

Tietoturva, tietosuoja, sopimuspalokunta

Luottamuksellisuus

julkinen

SAVONIA UNIVERSITY OF APPLIED SCIENCES

Degree Programme

Fire Officer (Engineer)

Author

Marko Heikkilä

Title of Project

Information Security and Data Protection of the Contract Fire Brigades in Oulu - Koillismaa Rescue Department

Type of Project	Date	Pages
Final Project	9 November, 2015	37+6

Academic Supervisor	Company Supervisor
Mrs. Mari Lyyra, Head Instructor	

Company

Abstract

The purpose of this final project was to find out how information security and data protection have been arranged for the contract fire brigade and part-time staff of Oulu-Koillismaa Rescue Department and how security training has been taken into account in training programs. The role of the contract fire brigade in rescue operations in the area of Oulu-Koillismaa Rescue Department is significant. In this area, there is permanent staff working 24 hours a day in Kuusamo, Oulu, Haukipudas and Kempele.

Data was collected with a questionnaire. Information security and data protection are broad concepts and therefore it was important to carefully formulate the questions concerning the operations of the contract fire brigades to get relevant answers. The questions were sent as a Webropol-questionnaire to all contract fire brigades and part-time fire-fighter units in the area of Oulu-Koillismaa Rescue Department. Additionally, the questionnaire was directed at the permanent staff that operates as trainers of the contract fire brigade and approve their training programs. In addition to the questionnaires, interviews were also conducted.

In terms of information security and data protection, it is notable that the operations where contract fire brigades are most often needed are first response operations and traffic accidents. In other words, operations where there is plenty of information about people available. For this reason, it is important that data protection and information security training is arranged. This final project pointed out the fact that not enough training has been organized and the matter should be better acknowledged when preparing training programs. Highlighting this matter was appreciated by the respondents.

Keywords

information security, data protection, contract fire brigades

Confidentiality

public

SISÄLTÖ

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on selvittää, miten sopimuspalokuntien ja sivutoimisen henkilöstön tietoturva ja tietosuoja ovat järjestetty ja miten koulutus on huomioitu Oulu-Koillismaan pelastusliikelaitoksella. Aiheena tietoturva on laaja, joten tarkoituksenmukaista on selvittää se, mikä tietoturvassa koskettaa sopimuspalokuntatoimintaa.

Tietoturvasta huolehtiminen kuuluu työnantajan toimenkuvaan ja tarvittaessa myös erilaiseen harrastustoimintaan, jossa saadaan sellaista tietoa, joka kuuluu tietoturvan tai tietosuojanpiiriin. Sopimuspalokuntatoiminta on hyvä esimerkki siitä, että tietoturvasta huolehtiminen ja kouluttaminen kuuluvat kyseiseen harrastustoimintaan siten, että tietoturvakoulutusta tulisi järjestää harjoituksissa. Harjoituksissa ja erilaisissa pelastustehtävissä saadaan tietoa, jota ei ole tarkoitettu julkisuuteen. Tieto voi olla myös julkista. Koulutuksen järjestämisellä voidaan erottaa ja saada tietoa siitä, mikä on julkista tietoa ja mikä ei.

Erilaisissa työpaikoissa järjestetään jo tietoturvakoulutusta siten, että saa suorituksen, että on suorittanut tietoturva-ajokortin. Samanlaista asiaa voisi miettiä myös sopimuspalokuntalaisten ja sivutoimisten henkilöstön koulutuksiin.

Tietoturvaan liittyen tietosuoja yhdistetään helposti samaksi asiaksi, vaikka kyseessä on kaksi eri asiaa. Kuitenkaan ilman kunnollista tietoturvaa ei voi olla kunnollista tietosuojaa ilman kunnollista tietosuojaa ei voi olla toimivaa tietoturvaa.

Tietoturvassa tarkoituksena on suojata tietoja ja tietojärjestelmiä ja samalla on tarkoitus varmistaa, että järjestelmät toimivat kaikissa olosuhteissa luottamuksellisina, eheinä ja ovat saatavilla. Tietosuojalla pyritään takamaan ihmisten yksityisyydensuoja, ettei tarpeeton tieto ole saatavilla. Kyseessä on ihmisten henkilötiedot, jotka ovat tietosuojan kohteena. (Järvinen 2012, 12.)

Aiheena opinnäytetyö on ajankohtainen. Erilaiset tietoturvaan liittyvät riskit ja uhat ovat jokapäiväistä elämäämme, ja onhan asia välillä esillä myös julkisuudessa. Työpaikoillamme on oltava jatkuva valmius, miten näitä riskejä ja uhkia voidaan minimoida. Usein luullaan, että tietoturva on ainoastaan tietokoneita tai tietoverkkoja koskevaa huolehtimista, mutta se on paljon muutakin. Tämä näkyy sopimuspalokuntatoiminnassa siten, että sopimuspalokuntalaisten tärkeimmät toimintamuodot ovat harjoituksiin ja hälytyksiin osallistuminen. Tällöin heidän toimintansa liittyy paljon muuhunkin, kuin tietokoneisiin tai tietoverkkoihin.

Pelastuslain (379/2011) 86 §:n mukaan pelastustoimen palveluksessa oleva tai pelastustoimintaan osallistuva ei saa pelastustoimeen kuulumattomalla tavalla käyttää hyödykseen eikä luvatta ilmaista muille tässä tehtävässä tietoon saamaansa seikkaa, jos siitä on laissa säädetty salassapitovelvollisuus tai asia koskee yksityistä liike- tai ammattisalaisuutta, terveydentilaa, taloudellista asemaa tai henkilökohtaista olosuhdetta.

2 TUTKIMUKSEN TOTEUTUS

Tässä opinnäytetyössä tutkimusmenetelmiksi valittiin haastattelut ja kyselyt. Kysely toteutettiin Webropol–järjestelmän kautta ja lähetettiin sähköisessä muodossa.

Tutkimusta tehtäessä on tutkimuksella aina jokin tehtävä tai tarkoitus. Tarkoitus tutkimuksessa ohjaa valintoja, ja tarkoitta sitä, miten tutkimusta on tarkoitus selvittää. Tutkimuksen tarkoitus voi olla kartoittava, selittävä, kuvaileva tai ennustava. Huomioitavaa on se asia, että tutkimuksessa voi olla useita tarkoituksia ja tutkimuksen aikana voi tarkoitus myös muuttua. (Hirsjärvi ym. 2005, 128 -130.) Tässä opinnäytetyössä tutkimuksen tarkoitus on selittävä ja kuvaileva. Eli löytää näiden kautta vastaus tutkimusongelmaan.

Selittävän tutkimuksen toiminnat ja asenteet vaikuttavat tutkimuskysymykseen. (Hirsjärvi ym. 2005, 129.) Tällä pystytään miettimään tässä opinnäytetyössä, miksi tietoturvakoulutus ja myös tietosuojakoulutus ovat jääneet vähäiselle huomiolle.

Selittävän tutkimuksen tarkoituksena on löytää ja etsiä tilanteeseen ja ongelmaan selitys. Tutkimuksen tyyppinä voi olla kvantitatiivinen, kvalitatiivinen ja kenttätutkimus. (Hirsjärvi ym. 2005, 129.)

Kuvailevan tutkimuksen tarkoituksena on esittää erilaisia tapahtumia ja tilanteita ja tarkkoja kuvauksia henkilöistä sekä tallentaa keskeiset ilmiöt ja mielenkiintoiset piirteet asiasta. Tällaisen tutkimuksen strategiana voi toimia laadullinen tai määrällinen tutkimus, kenttätutkimus tai survey-tutkimus. (Hirsjärvi ym. 2005, 130.) Kuvailevan tutkimuksen perusteella, kun on tehty kyselytutkimus, saadaan vastauksia tilanteisiin, millainen on tietoturvan ja tietosuojan taso, miten se on huomioitu koulutuksessa sekä uusia jäseniä mukaan otettaessa.

Tietoa tietoturvasta ja tietoturvakoulutuksesta on ollut vähän Oulu–Koillismaan pelastuslaitos alueen sopimuspalokuntalaisille. Tämän vuoksi voisi todeta, että aiheena asia on vähemmän tiedetty. Opinnäytetyössä on tarkoitus nostaa kyseinen asia esille.

Tutkimusstrategiana on kolme perinteistä tapaa. Tässä opinnäytetyössä käytettiin yhtenä tutkimusmenetelmänä survey–tutkimusta, siinä tietyltä joukolta kerätään tietoa standardoidussa muodossa ja tapaustutkimus, joka on tarkkaa, intensiivistä tietoa jostain yksittäisestä tapauksesta tai pienestä määrästä suhteessa toisiinsa olevia tapauksia. (Hirsjärvi ym. 2005, 125.)

Kyselytutkimus toteutetaan survey–tutkimuksena. Tyypillisiä piirteitä tällaiselle kyselytutkimukselle on, että valitaan tietystä ihmismäärästä otos henkilöitä, käytetään kyselylomaketta, joka lähetetään ennakkoon valituille henkilöille, kerätään aineisto jokaiselta henkilöltä strukturoidussa muodossa eli muodossa, jossa kyselyn kysymykset ja vastausvaihtoehdot ovat etukäteen tarkasti määritelty ja saadun aineiston perusteella pyritään kuvailemaan, vertailemaan ja selittämään ilmiötä, mihin on haluttu saada vastaus. (Hirsjärvi ym. 2005, 125.) Tein kysymyspatteriston ja lähetin ne sähköisesti valituille henkilöille, joita sain pelastuslaitoksen ja omien kontaktien kautta.

Aina ei mainita tai puhuta otoksesta, joka otetaan mukaan tutkimukseen tai kyselyihin, silloin kvalitatiivisessa eli laadullisessa menetelmässä kerrotaan harkinnanvaraisesta näytteestä, koska tarkoitus on pyrkiä ymmärtämään joitakin tapahtumia paremmin, saamaan lisätietoa ilmiöstä tai asiasta, jotka koskettavat paikallista ilmiötä tai löytää uusiin tapahtumiin ja näkökulmiin uusia erilaisia teoreettisia näkökulmia. Tällöin muutamaa henkilöä haastattelemalla voidaan saada merkittävää tietoa. (Hirsjärvi, Hurme 2008, 59.)

Tässä opinnäytetyössä Webropol–kyselyn lisäksi tein haastatteluja. Tämä tuli eteen, kun en saanut niin paljoa vastauksia Webropol–kyselyjen kautta kuin odotin, vaikka sitäkin kautta vastausprosentti oli hyvä. Tällöin haastattelut ovat myös hyvä vaihtoehto etsiä vastauksia omaan tutkimusongelmaan.

Laadullisen tutkimuksen tyypillisiä piirteitä ovat esimerkiksi tilanteet, joissa tietoa hankitaan todellisissa tilanteissa ja tietoa saadaan, kun tiedon hankinta on kokonaisvaltaista asian suhteen. Samoin tiedonvälineenä käytetään ihmistä. Laadulliseen tutkimukseen kuuluu myös erilaisten menetelmien käyttö selvitettäessä tutkimusongelmaa. Lisäksi tutkimukseen valitut henkilöt on valittu tarkoituksenmukaisesti, ei sattumanvaraisesti.

Opinnäytetyössä on valittu tarkasti, kenelle kysymyksiä on lähetty Webropol-kyselyn kautta ja ketä on sen lisäksi haastateltu. Myös se asia on huomioitava, että kun tutkimussuunnitelma on tehty tutkimusongelmasta tai asiasta, jota on tarkoitus selvittää, tutkimuksen edetessä muotoutuu myös tutkimussuunnitelma. (Hirsjärvi ym. 2005, 155.)

Kun tein Webropol-kyselyä ja haastatteluja, sain kontaktit omien kontaktien sekä pelastuslaitoksen kautta. Kun tehdään kyselyä tai haastattelua, se perustuu pääsääntöisesti survey-tutkimuksen kyselyihin ja haastatteluihin. (Hirsjärvi, Hurme 2008, 58.)

Kyselyissä voi tulla ongelmaksi vastausten saaminen. Helposti vastaukset jäävät 30 - 40 prosentin tuntumaan. Kuitenkin vastausprosenttia voidaan odottaa korkeammaksi, jos kyselyt on tehty jollekin erityisryhmälle ja asia koskettaa vastaajia hyvinkin paljon. (Hirsjärvi ym. 2005, 185.)

Kvalitatiivisessa tutkimuksessa haastateltavien henkilöiden määrä voi vaihdella, ja näin ollen se voi helposti olla liian pieni tai suuri. Kun halutaan, että näiden ero ei ole liian suuri, on päädytty siihen, että kvalitatiivisessa tutkimuksessa näyttää nykyisin olevan keskimäärin 15 henkilöä haastateltavina. (Hirsjärvi, Hurme 2008, 58.)

Lähetin kysymykset alueen kaikille sopimuspalokunnille sekä sivutoimiselle henkilöstölle. Lisäksi tein syvempiä haastatteluja muutamille henkilöille, joita sain kiinni. Henkilöt osallistuivat ja vastasivat myös Webropol-kyselyyn.

Mielestäni vastaukset, joihin olen saanut vastaukset opinnäytetyöhön liittyen, ovat luotettavia, eli tutkimuksen reliabiliteetti toteutuu, koska vastaajat edustavat yli puolia alueen sopimuspalokuntalaisia tai sivutoimista henkilöstöä ja vastaukset ovat yhteneväisiä. Lisäksi voisi todeta, että jos kysely toistettaisiin, olisivat vastaukset ja tulokset todennäköisesti samanlaisia.

Mikäli halutaan tutkimuksessa osoittaa tutkimuksen reliabiliteetti, se vaatii samalta henkilöltä tutkimukseen kahdella eri kerralla saman vastauksen ja tuloksen (Hirsjärvi, Hurme 2008, 185). Tässä opinnäytetyössä tehtiin kaksi erillistä kyselyä. Niiden vastauksista pystyi päättelemään sen, että vastaukset ovat yhteneviä.

Tutkimukseen liittyy myös validiteetti eli käsitteenä validius, joka tarkoittaa pätevyyttä siihen, miten tutkimusmenetelmä tai mittarin on tarkoitus mitata nimenomaan sitä tutkimusongelmaa, joka on tarkoitus esimerkiksi mitata tai ratkaista (Hirsjärvi ym. 2005, 216). Tutkimuksessa validius pyrittiin saamaan aiemman kokemuksen tiedon perusteella. Validius tarkoittaa luotettavuutta ja paikkaansapitävyyttä. Vaikka kyselyssä oli vaihtoehtoväittämiä, oli kyselyssä myös avoimia kysymyksiä, joihin vastaajat saivat kertoa omia näkemyksiä. Tämä antaa mahdollisuuden vastaajille kertoa jostain kysymyksestä tarkemmin oman näkökulman asioihin. Tällöin vastauksiin ei ole olemassa yhtä totuutta, vaan vastaajilla voi olla erinäkemyksiä asioihin. Vaihtoehtokysymyksissä kysymykset ovat muodoltaan sellaisia, että niihin riittää vastaukseksi kyllä tai ei. Vastauksissa ei jää silloin ainakaan tulkinnanvaraa, vaan helposti näkee asiaan muodostetun kannan.

On olemassa myös mahdollisuus, joka heikentää tutkimuksen validiutta. Vaihtoehtoväittämiin ei tutkija voi vaikuttaa ja kontrolloida, miten vastaajat ovat ymmärtäneet kysymykset. Lisäksi on huomioitava se, kuinka vakavasti vastaajat ovat suhtautuneet kyselyyn ja kuinka huolellisesti tai avoimesti ovat vastanneet. (Hirsjärvi ym. 2005, 184.)

Olen ollut mukana sopimuspalokuntatoiminnassa aikana ennen aluepelastuslaitoksia. Silloin ei tietoturvasta ja tietosuojasta ollut mitään puhetta tai siitä mitä ne tarkoittavat. Toki yhteiskunta on niistä ajoista muuttunut paljon. Kysymyksiä tehdessäni on tietoa tullut tietoturvaan ja tietosuojaan paljon lisää verrattuna siihen aikaan, kun oli mukana sopimuspalokuntatoiminnassa. Kuitenkin on tiedossa ne asiat, jotka vaikuttavat eniten tähän asiaan. Oma näkökulmani kysymyksiin syntyi, kun näin harjoittelussa, miten sopimuspalokuntalaisten näkökulmasta asiaa on hoidettu. Tutkimalla lainsäädäntöä ja havainnoimalla paikan päällä sain selville, mitä kannattaa kysyä. Muutamalle henkilölle lähetin kyselyn ennen varsinaista kyselyä, ja nämä henkilöt eivät toimineet Oulu-Koillismaan pelastuslaitoksen palveluksessa tai sopimuspalokunnissa. Heidän mielestään kysymystenasettelut ovat riittävät.

3 TIETOTURVA JA TIETOSUOJA

Usein tietoturva ja tietosuoja menevät ihmisten mielessä sekaisin, koska ne muistuttavat termeinä toisiaan läheisesti. Helposti asiat voivat mennä sekaisin, jos ei ole perehtynyt, mitä termit tarkoittavat. Tämä koskettaa kaikkia ihmisiä, joille tietoturva- ja tietosuoja-asiat ovat jääneet vähäiselle huomiolle tai koulutukselle. Kyse on molemmissa termeissä tietojen suojaamisesta, mutta sisältönä ne ovat erilaisia, koska tietojen sisältö ja tarkoitus suojata tietoa ovat erilaisia (Järvinen, 2012, 12).

Tietoturvaa parantamalla parannetaan myös tietosuojaa. Nämä asiat täydentävät ja liittyvät läheisesti toisiinsa. Teknisillä ja erilaisilla toiminnallisilla järjestelyillä voidaan parantaa ja lisätä tietoturvaa, jolloin on mahdollisuus myös parantaa tietosuojaa. (Järvinen, 2002, 21.)

3.1 Tietoturva

Aiheena tietoturva on laaja. Tavoitteet tietoturvan toiminnalle ovat sellaiset, että tiedon täytyy pysyä luottamuksellisena, tietojen täytyy säilyä eheinä ja tietojen täytyy olla saatavilla tarvittaessa. (Järvinen 2012, 10.)

Luottamuksellinen tieto saa olla ainoastaan niillä henkilöillä, joita asia koskettaa. Julkisuuteen ei saa tulla sellaisia tietoja henkilöstä, jotka koskevat henkilötietoja yksityiselämän suojasta tai koskettavat yrityssalaisuuksia. (Järvinen 2012, 10.)

Lain viranomaisten toiminnasta julkisuudessa (621/1999) 6 luvussa määritellään salassapitovelvoitteista. Luvussa on määritelty ne asiat, jotka koskevat asiakirjajulkisuutta, vaitiolovelvollisuutta ja hyväksikäyttökieltoa, salassa pidettäviä viranomaisen asiakirjoja ja salassapito-tai luokitusmerkintöjä.

Lisäksi käytön tai tiedonkäsittelyn aikana oikeutettuja muutoksia sallitaan ainoastaan tiedon kohdistumiseen. Tietoturvaongelmana voidaan mainita virukset, joita voi tulla sähköpostien välityksellä, näin ollen viesti ei ole enää alkuperäisessä muodossa ja toimi eheyden periaatteella. (Järvinen 2012, 10.)

Käytettävyydessä koneiden täytyy olla saavutettavissa, että niitä voidaan käyttää silloin, kun niitä tarvitaan. Samoin tietojen ja palvelun on toimittava, kun niitä tarvitaan. Tämä

tuo erilaisia haasteita, koska välillä voi koneita mennä rikki, sovellukset eivät toimi ja nettiyhteydet pätkivät eri syistä. (Järvinen 2012, 10.)

Usein tietoturvaongelmat johtuvat todentamisen vaikeudesta. Haasteen asiaan tuo se, miten tunnistetaan ja varmistetaan henkilötiedot, saadaan varmuus verkkopalveluiden aitoudesta ja laitteista. (Järvinen 2012, 12.)

Tietoturva täytyy ottaa kuitenkin vakavasti, se täytyy suhteuttaa mahdollisiin uhkien vakavuuteen, tekniseen tasoon, siihen mihin ollaan sitouduttu, ja kustannuksiin. Tällainen vaatimus tarkoittaa sitä, että mikäli on tiedossa tietoturvaan liittyviä uhkia, tulee varautua uskottavasti mahdollisiin tietoturvaongelmiin. (Helopuro, Perttula ja Ristola 2004, 145.)

Organisaatioiden omaan toimintaan ja yhteiskunnan toimintaan sekä henkilötietoihin liittyviä tietoja suojataan tietoturvallisuudella. Julkishallinnon eri organisaatioiden keskeinen osa on oikeat ja luotettavat tiedot, joilla on vaikutusta päätöksentekoon ja toimintavarmuuteen. (Andreasson ja Koivisto 2013, 32.)

Tietoturva voidaan jakaa eri osa-alueisiin.

1. Hallinnollinen turvallisuus

Perusta tietoturvallisuuteen luodaan hallinnollisen tietoturvallisuuden kautta organisaatioissa. Tietoturvasta huolehditaan tehtäessä riskienarviointia, jolloin organisaatioissa voidaan tunnistaa ja arvioida sekä hallita tietoturvauhkia, joilla on merkitystä toiminnassa. Tavoite on lisätä tietoturvatietoisuutta. Tietoturvapolitiikan järjestely ja kehittäminen lähtevät liikkeelle organisaation johdosta. Hyvä tietoturvapolitiikka edellyttää säännöllisin väliajoin riskien seuraamista ja arviointia, jotta voidaan tarvittaessa saada tietoa, miten tietoturvapolitiikka on toiminut ja löytyykö tarpeita kehittää toimintaa. Näin voidaan tarvittaessa tehdä erilaisia parannusehdotuksia tietoturvan kehittämiseksi. (Kokkala 2010, 6)

Tietoturva on organisaation johdon hyväksymää tietoturvapolitiikkaa. Se lähtee organisaation omista tavoitteista, päämääristä, periaatteista ja toteuttamistavoitteista, jotka johto on hyväksynyt. Huomioitavaa on se asia, että tietoturvapolitiikkaa koskettaa koko organisaatioon kuuluvaa henkilöstöä, ei ainoastaan johtoa. (Järvinen 2002, 113.)

Hallinnollisen tietoturvan toimintatavat ovat yleisen tietoturvan huolehtiminen, vastuunjako ja toiminnan organisointi (Järvinen 2002, 112).

2. Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella voidaan tarkoittaa esimerkiksi sitä, että huolehditaan turvallisesta käsittelystä sekä järjestetään tietoaineistot tietojen käsittelyn mukaisesti, huolehditaan turvallisesta säilytyksestä, että on kaikenlaiset tärkeät asiakirjat ja yksittäiset tiedot suojattu (Helopuro ym. 2004, 147). Tietoaineistoturvallisuuden kannalta lainsäädännöllä on merkitystä. Julkisuuslaki on tässä se, joka ohjaa tietoaineistoturvallisuutta.

Lisäksi tietoaineistoturvallisuuteen kuuluu erilaisia toimenpiteitä, kuten tietojen säilyttämiseen, varmistamiseen, palauttamiseen ja tuhoamiseen liittyviä toimia. Yleensä tietohallinto vastaa tietoaineturvallisuudesta. (Hakala ym. 2006, 11.)

3. Henkilöstöturvallisuus

Henkilöstöturvallisuuden kannalta riskien arviointi alkaa jo rekrytoinnin aikana, kun uudelle työntekijälle on mahdollista tehdä erilaisia taustaselvityksiä sekä turvallisuusselvityksiä. Näin pyritään parantamaan henkilöstöön kohdistuvaa henkilöstöturvallisuutta. (Valtionvarainministeriö 2006, 48.) Uusi turvallisuusselvityslaki astui voimaan vuoden 2015 alussa. Tämän selvityksen johdosta voidaan karsia tarvittaessa henkilöitä rekrytointivaiheessa, mikäli selvitys tehdään ja selvityksen hakija on sitä mieltä, että sillä on merkitystä.

Lisäksi kannattaa järjestää uusille työntekijöille ja toimintaan mukaan tuleville perehdyttämiskoulutusta tietoturvasta. On muistettava, että jossain vaiheessa jonkun henkilön jäädessä pois toiminnasta, on erityisen tärkeää muistuttaa ja ohjeistaa tilanteesta, miten silloin toimitaan. (Järvinen 2002, 112.)

Henkilöstöturvallisuus on riskienhallintaa, joka koskee koko henkilöstöä. Henkilöstöturvallisuuden osalta voidaan arvioida henkilön soveltuvuutta, tiedonsaanti-ja käyttöoikeutta sekä toimenkuvaa. (Valtionvarainministeriö 2008, 19.) Tällöin täytyy esimerkiksi määritellä, kenellä ja millä periaatteella tai ryhmillä on tietojen haltuun saaminen ja lupa käsitellä tietoja, ketkä pääsevät käyttämään palvelimia eli saavat olla tietoverkoissa ja kenellä on oikeus päästä tiloihin, joissa toimintaa harjoitetaan. (Valtionvarainministeriö 2008, 27). Organisaatiossa pääsääntöisesti henkilöstöhallinto yhdessä tietohallinnon ja muiden turvallisuudesta vastaavien kanssa huolehtii henkilöstöturvallisuudesta (Hakala ym. 2006).

4. Käyttöturvallisuus

Käyttöturvallisuudessa ihmisen toiminta on merkittävä. Esimerkiksi käyttöoikeutta saa antaa vain niihin kuuluviin tehtäviin. Pelastuslaitoksilla on mietittävä, kenelle voidaan myöntää Pronto-tunnukset. Lisäksi salasanat ja niiden tarpeeksi usein vaihtaminen on välttämätöntä. On huomioitava se, millaiset vähimmäisvaatimukset ylläpitäjä vaatii salasanoista. Kuitenkin kun käytetään erilaisia ohjelmia, esimerkiksi Prontoa, aina jää lokitiedostoon tieto, mitä siellä on tehty. Pelastuslaitoksille on nimetty Pronton pääkäyttäjä, hänelle on nimettävä varahenkilö. Suositellaan myös välillä henkilöiden kierrättämistä eri tehtävissä, jos se on vain mahdollista organisaatiossa.

Nykyisin ei tietokoneita ja tietoverkkoja käytetä pelkästään toimistoissa. Pelastusajoneuvot ovat myös tietoverkoissa. Tämä lisää valvontaa myös tietoturvan osalta. Näitä laitteita voidaan pitää aktiivilaitteina, jolloin aktiivilaitteisiin kuuluu turvata päivittäinen laitteiden turvaaminen, miten on huolehdittu käytöstä, huollosta, valvonnasta tai miten laitteita ylläpidetään (Järvinen 2002, 113).

5. Tietoliikenneturvallisuus

Tietoliikenneturvallisuus tarkoittaa esimerkiksi sitä, että erilaisten viestintäverkkojen avulla liikkuvat tiedot tai viestit eivät tule koskaan ulkopuolisten tietoon ja ulkopuoliset henkilöt eivät pääse käsiksi viesteihin muuttamalla tai tuhoamalla niitä. Lisäksi täytyy voida estää ulkopuolisten mahdollisuus päästä tunnistamistietoihin tai käsittelyä koskeviin tietoihin. Mikäli haluaa päästä tietoliikennettä koskeviin asioihin käsiksi, täytyy löytyä riittävät todentamismenettelyt, pääsynvalvontatiedot ja kiistämättömyysmenettelyt. (Helopuro ym. 2004, 146 – 147.) Vastuu tietoliikenneturvallisuuden toiminnasta kuuluu organisaation tietohallinnolle. (Hakala ym. 2006, 12).

6. Fyysinen turvallisuus

Valtionhallinnon tietoturvasanaston Vahti 8/2008 mukaan fyysisellä turvallisuudella tarkoitetaan ”henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaamista tuhoja ja vahinkoja vastaan. Sanaston mukaan fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden”. (Andreasson ja Koivisto 2013, 52 – 53.)

Toimitilojen fyysistä turvallisuutta ei pidä vähätellä. On todettu, että erilaisilla turvaratkaisuilla ei ole merkitystä, jos fyysinen turvallisuus ja suojaus eivät ole ajan tasalla. (Järvinen 2002, 112.)

3.2 Tietosuoja

Säädösperustana yksityiselle tietosuojalle voidaan pitää lakia yksityisyyden suojasta työelämässä (759/2004), henkilötietolakia (523/1999), lakia viranomaisten toiminnasta julkisuudessa eli julkisuuslaki (621/1999). (tietosuojavaltuutetun toimisto 2015.)

Tietosuojaa voidaan kutsua myös yksityisyyden suojaksi. Tietosuoja tarkoittaa ”henkilötietojen sekä henkilökohtaiseen toimintaan liittyvien tietojen keräämisen ja käsittelyn rajoittamista niin, ettei henkilön yksityisyys vaarannu. Käsite on noussut esille, kun on huomattu, kuinka helpoksi ja tehokkaaksi tietojen kerääminen on tekniikan myötä käynyt”. (Järvinen 2002, 21.)

Henkilötietolain, sähköisen viestinnän tietosuojalain ja lain yksityisyyden suojasta työelämässä mukaan tietyssä asemassa olevat henkilöt, jotka saavat tietoja ihmisistä, eivät saa paljastaa tai ilmaista niitä muille. Näihin lakiin on kirjattu vaitiolo- ja salassapitovelvollisuus, joten kyse on tietosuojasta, joka koskee yksityisyyttä ja yksityiselämän suojaa parantavasta tietosuojasta. (Pesonen 2012, 15.)

Yksityisyyden suojalle ei kuitenkaan valvonta ja seuranta ole haitaksi. On hyvä seurata, miten viranomaiset käyttävät saamiaan oikeuksia tietojen keräämiseen tai käsittelyyn. Tietojärjestelmiä käytettäessä voidaan viranomaisten ja myös tavallisten ihmisten tekemiset tietoverkossa tallentaa ja rekisteröidä, koska mahdollisten väärinkäytösten selvittäminen helpottuu tätä kautta. Lain puitteissa eri viranomaisilla on oikeus kerätä henkilöistä tietoja ja käsitellä niitä. (Järvinen 2002, 30.)

Esimerkiksi Prontoon tehdään merkintöjä ihmisistä. Kun Prontoon kirjaudutaan, jää aina jälki siitä, kuka ja milloin on kirjautunut. Prontossa on esimerkiksi tietoja henkilöistä, jotka henkilötietolain 523/1999 mukaan on salassa pidettävää. Mikäli tulisi jokin riitatapaus, jolla on merkitystä henkilötietolain mukaisesti tietosuojasta, voi käsitelty tieto, joka on tallennettu ja kerätty, koitua henkilön omaksi eduksi ja turvaksi.

Henkilötieto koskee luonnollista henkilöä, hänen elämänolojaan tai hänen ominaisuuksiaan koskevaa tietoa. Tieto jonka on oltava suojattua voi koskea myös niin perhettä tai muuten samassa taloudessa asuvia henkilöitä. (Pesonen 2012, 16.)

Henkilötiedon muoto voi olla kuvallisessa muodossa tai tekstinä. Myös numeerinen tieto voi olla henkilötietoa. Erilaiset tiedot henkilöstä, esimerkiksi tulot, varallisuus, terveydentila ja perhesuhteet, ovat henkilötietoja. Voidaan todeta, että tieto saa henkilötiedon luonteen silloin, kun se kuvaa henkilöä tai yksilöä yhdistelemisien kautta. Henkilötieto on oltava tallennettuna jossain asiakirjassa tai tiedostossa, jotta voidaan todeta, että kyseessä on lain tarkoittama henkilötieto, koska suullinen tieto ei ole sitä lain tarkoittamassa mielessä. (Pesonen 2012, 16 – 17.)

Laissa yksityisyydensuojasta työelämässä noudatetaan säännöksiä henkilöistä, jotka ovat työsuhteessa tai virkasuhteessa ja siihen verrattavassa julkisoikeudellisessa palvelusuhteessa. Laissa säädettäessä työntekijästä, koskevat heitä samat säännökset ja niitä sovelletaan myös virkamiehiin ja virkasuhteissa toimiviin henkilöihin sekä niihin verrattavissa julkisoikeudellisissa palvelusuhteissa toimiviin henkilöihin. Tässä laissa tarkoitetaan myös työntekijällä henkilöä, joka voi työsuhteella tarkoittaa muutakin palvelusuhdetta. (Korhonen 2003, 132.)

Julkisuuslain eli lain viranomaisten toiminnan julkisuudesta (621/1999) koskee kaikkia viranomaisia Suomessa. Pelastuslaissa 379/2011 on määritelty sen 86§.ssa vaitiolovelvollisuudesta, joka koskee pelastustoimea. Tämä lain kohta uudistui maaliskuussa 2015.

Uusi lakipykälä on 281/2015. Siinä kerrotaan, seuraavaa: ”Salassa pidettävän tiedon ilmaisemisesta viranomaiselle tai julkista tehtävää hoitavalle toimielimelle säädetään lailla. Vaitiolovelvollisuus ei estä ilmaisemasta sellaista tietoa, jonka ilmaiseminen on yksittäistapauksessa tarpeen hengen tai terveyden suojaamiseksi tai huomattavan ympäristö- tai omaisuusvahingon välttämiseksi. Salassapitovelvollisuuden estämättä tarkoitetuilla henkilöillä on myös oikeus ilmoittaa poliisille henkeen tai terveyteen kohdistuvan uhkan arviointia ja uhkaavan teon estämistä varten välttämättömät tiedot, jos hän tehtäviä hoitaessaan on saanut tietoja olosuhteista, joiden perusteella hänellä on syytä epäillä jonkun olevan vaarassa joutua väkivallan kohteeksi” (Pelastuslaki 379/2011, 86§.)

Julkisuuslain mukaan salassa pidettävää tietoa, joka koskee pelastustoimea, on esimerkiksi, viranomaisen asiakirja, joka on pidettävä salassa, jos se tässä tai muussa laissa on

säädetty salassa pidettäväksi tai jos viranomainen lain nojalla on määrännyt sen salassa pidettäväksi taikka jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus. Salassa pidettävää viranomaisen asiakirjaa tai sen kopiota tai tulostetta siitä ei saa myöskään näyttää eikä luovuttaa sivulliselle eikä antaa sitä teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi (Laki viranomaisten toiminasta julkisuudesta 621/1999, 22 §.)

Henkilötietolain 523/1999 mukaan lain tarkoituksena on toteuttaa yksityiselämän suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä ja edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista (Henkilötietolaki 523/1999, 1 §).

Arkaluontoista tietoa on lain mukaan kielletty käsitellä. Henkilötietoja, jotka ovat arkaluontoisia ja kuvaavat henkilötietoja, ovat esimerkiksi rotua tai etnistä alkuperää, henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista, rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta, henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia, henkilön seksuaalista suuntautumista tai käyttäytymistä, taikka henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia. (Henkilötietolaki 523/1999, 11 §.)

4 TIETOTURVA SOPIMUSPALOKUNNASSA

Pelastuslain nro 25 §:n mukaan pelastustoimen tehtävien hoitamista varten täytyy olla pelastuslaitos omalla pelastustoimialueella. Alueen pelastustoimi voi käyttää pelastustoiminnassa lain 32 §:n mukaan apunaan vapaaehtoista palokuntaa, teollisuuspalokuntaa, laitospalokuntaa, sotilaspalokuntaa tai muuta pelastusalalla toimivaa yhteisöä siten, miten asiasta on sovittu. Pelastuslain 32 §:n mukaan pelastustoimintaan kuuluvia tehtäviä ovat hälytysten vastaanottaminen, väestön varoittaminen, uhkaavan onnettomuuden torjuminen, onnettomuuden uhrien ja vaarassa olevien ihmisten, ympäristön ja omaisuuden suojaaminen ja pelastaminen, tulipalojen sammuttaminen ja vahinkojen rajoittaminen sekä edellä mainittuihin tehtäviin liittyvät johtamis-, viestintä-, huolto- ja muut tukitoiminnot.

Sopimuspalokuntatoiminnassa lähtökohtana tietoturvaan ja tietosuojaan on pelastuslain 379/2011, 86 §, joka määrittelee salassapitovelvollisuudesta, tiedonsaantioikeudesta ja henkilörekistereistä. Kuitenkin tietoturvaa ja tietosuojaa voidaan avata tarkemmin erilaisilla lainsäädännöillä, joilla on merkitystä sopimuspalokuntatoimintaan. Tietoturvan kannalta kannattaa huomioida lait, joilla on merkitystä sopimuspalokuntatoimintaan. Vaikka on olemassa laki pelastustoimesta, joka koskee salassapitovelvollisuutta, on voimassa laki yksityisyydensuojasta työelämässä, henkilötietolaki, laki viranomaisten toiminnasta julkisuudessa, turvallisuusselvityslaki ja rikoslaki.

4.1 Tietoturvalainsäädäntö

Lakia yksityisyydensuojasta työelämässä sovelletaan 2 §:n mukaan siten, mitä tässä laissa säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista ja teknisestä valvonnasta työpaikoilla. Tekninen valvonta voi olla esimerkiksi sähköistä kulunvalvontaa paloaseman tiloissa. Useimmiten tätä lakia sovelletaan, kun ollaan rekrytoimassa uusia jäseniä mukaan toimintaan tai säännöllisin väliajoin tehdään testaukset, ja joilla pyritään osoittamaan, että on esimerkiksi terveydentilan vuoksi mahdollinen jatkamaan toiminnassa. (Laki yksityisyydensuojasta työelämässä 759/2004.)

Sopimuspalokuntalaiset tekevät omasta toiminnastaan sammutussopimuksen. Siinä määritellään heidän tehtävänsä siitä, mitä on sovittu pelastuslaitoksen kanssa ja mitkä kuuluvat tehtäviin. Silloin siitä saadut tiedot ovat salassa pidettäviä, ellei laki toisin sano. Tämä kuitenkin vaatii tietoturva ja tietosuojakoulutusta.

Henkilötietolain 523/1999 mukaan henkilöistä voidaan kerätä henkilötietoja toimiessaan sopimuspalokunta toiminnassa. Henkilötietolain 3 §:n 4momentin mukaan rekisterinpitäjällä tarkoitetaan yhtä tai useampaa yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty.

Pelastuslaitos toimii omalla pelastustoimen alueella rekisterinpitäjänä, joten se vaatii rekisterinpitäjältä suurta huolellisuutta, etteivät henkilötiedot leviä eteenpäin. Myös sopimuspalokunnat voivat toimia rekisterinpitäjänä yhdistyksensä kautta.

Laki viranomaisten toiminnasta julkisuudessa koskee viranomaisia, jotka on määritelty lain 4 §:ssä. Tämän pykälän mukaisesti sopimuspalokuntalaiset eivät ole viranomaisia, mutta heitä koskee tämän lain 23 §, jossa mainitaan vaitiolovelvollisuudesta. Näin ollen viranomaisen palveluksessa oleva ei saa paljastaa salassa pidettävää tietoa tai sisältöä, joka on määritelty salaiseksi, eikä muutakaan tietoa, jota on saanut tietoonsa vaitiolovelvollisuuteen liittyen. Samoin kun toiminta loppuu, jossa on saanut vaitiolovelvollisuuden piiriin kuuluvaa tietoa, ei tietoa saa levittää ja paljastaa eteenpäin. (Laki viranomaisen toiminnasta julkisuudesta 621/1999.)

Lain mukaan salassapitovelvollisuus koskee myös sitä, joka harjoittelijana tai muutoin toimii viranomaisessa tai viranomaisen toimeksiannosta tai toimeksiantotehtävää hoitavan palveluksessa tai joka on saanut salassa pidettäviä tietoja lain tai lain perusteella annetun luvan nojalla, jollei laista tai sen perusteella annetusta luvasta muuta johdu (Laki viranomaisten toiminnasta julkisuudesta 621/1999).

Lisäksi on tullut voimaan vuoden 2015 alussa uusi turvallisuusselvityslaki. Lain tarkoituksena on määritellä ja mahdollisuus toteuttaa henkilöturvallisuusselvitys. Tällä pyritään selvittämään henkilön luotettavuuden ja nuhteettomuuden varmistaminen siten, että henkilön katsotaan olevan sopiva toimimaan esimerkiksi pelastustoimen tehtävissä. Tällöin sopimuspalokuntalaisesta voidaan tehdä suppea henkilöturvallisuusselvitys, jonka tekee paikallispoliisi. (Turvallisuusselvityslaki 726/2014.)

Uusi turvallisuusselvityslaki antaa mahdollisuuden valita jäseniä sopimuspalokuntatoimintaan, mutta se ei sido kuitenkaan valitsemasta mukaan toimintaan henkilöitä, vaikka selvitys antaisi millaisen tahansa tuloksen henkilöstä. Päätöksen siitä, millaisen painoarvon turvallisuusselvitykselle antaa, tekee selvityksen hakija. Sopimuspalokunnalla on ilmoituksia esimerkiksi lehdissä, miten halutaan uusia jäseniä mukaan toimintaan. Lehdissä mainitaan jo, millaisia henkilöitä halutaan mukaan toimintaan. Nykyisen lain mukaan on mahdollisuus selvittää asia, ketä voidaan ottaa mukaan toimintaan, koska on tullut voimaan uusi turvallisuusselvityslaki. Kuitenkin täytyy muistaa se, että tehtäessä tai vaadittaessa turvallisuusselvitys, täytyy siihen olla toimintaan mukaan tulevan kirjallinen suostumus.

Kuitenkin on hyvä asia, että voidaan tehdä turvallisuusselvitys, mikäli halutaan, mutta se ei ole estänyt tapahtumasta sinällään ikäviä asioita sopimuspalokuntalaisten toiminnassa. Täytyy muistaa, että turvallisuusselvitys ei kuitenkaan kerro kaikkea henkilöstä, ja silloin voi tapahtua myös ikäviä asioita.

Pelastustoimen yksi arvoista on, että toimitaan luotettavasti. Tämä tarkoittaa myös sitä, että kun saadaan tietoon asioita, jotka ovat salassapitomääräysten alaisia, niitä noudatetaan. Pelastuslain nro 86 § koskee vaitiolovelvollisuutta.

Kuitenkin on olemassa seikkoja, jotka voivat edellyttää, että salassapitomääräystä joudutaan avaamaan. Lainsäädännöllä on tehty mahdolliseksi ilmaista salassa pidettävää tietoa viranomaiselle tai julkista tehtävää hoitavalle toimielimelle. Vaitiolovelvollisuudesta huolimatta on seikkoja, joita voidaan ilmaista. Tällainen voi olla, jossa on tarpeen hengen tai terveyden suojaamiseksi tai huomattavan ympäristö- tai omaisuusvahingon välttämiseksi. Lisäksi henkilöllä on oikeus ilmoittaa henkeen tai terveyteen koskevaa uhkaa tai arviointia poliisille tai uhkaavan teon estämistä varten välttämättömät tiedot, joita on saanut hoitaessaan tehtävää olosuhteista, jotka voivat aiheuttaa vaaraa siitä, että epäilee jonkun joutuvan väkivallan kohteeksi. (Pelastuslaki 379/2011.) Nämä asiat koskettavat pelastuslain mukaan toimintaan osallistuvia henkilöitä. Heillä on silloin tarpeeksi hyvä tieto asioista, jotka koskevat salassapitoa.

Pääsääntöisesti yksityiselämään kohdistuva lainsäädäntö kohdistuu tietoon, joka ei ole julkista ja saa jäädä ainoastaan viranomaisten ja asianosaisten tietoon. Mikäli salassapidossa olevaa tietoa halutaan avata, siihen on oltava perusteltu syy.

Rikoslain 40. luvun, 11 §:n mukaan virkamiehellä tarkoitetaan henkilöä, joka on virka- tai siihen rinnastettavassa palvelusuhteessa valtioon, kuntaan, kuntayhtymään tai muuhun kuntien julkisoikeudelliseen yhteistoimintaelimeen. Julkisyhteisön työntekijällä tarkoitetaan henkilöä, joka on työsopimussuhteessa edellä mainittuihin julkisyhteisöihin tai laitoksiin. Näin ollen sopimuspalokuntalaisiin, jotka ovat toimeksiantosuhteessa, tai sivutoiminen henkilöstö, joka tehnyt suoraan henkilökohtaisen työsopimuksen alueen pelastuslaitoksen kanssa, on verrattavissa henkilöön, jota tässä laissa tarkoitetaan.

Rikoslain 38. luku koskee seuraamuksia tieto- ja viestintärikoksista. Sopimuspalokuntalaisten näkökulmasta katsoen tässä laissa tapahtuvat väärinkäytökset, mikäli niitä tapahtuu, ovat asianomistajarikoksia. Näin ollen syyttäjä ei voi nostaa syytettä, ellei asianomistaja sitä tai yleinen etu vaadi. Se, että jos tapahtuu jotain, mikä voi olla rangaistavaa lainsäädännöllisesti ja mitä siitä seuraa, koskee kaikkia pelastustoimintaan osallistuvia henkilöitä, myös sitä sivutoimista henkilöstöä, joka osallistuu hälytyksiin ja on kenties asemalla varikkovalmiudessa sekä saavat tällöin tietoonsa arkaluontoista tietoa.

4.2 Ongelmia lain soveltamisessa

Tietoturva perustuu vapaaehtoisuuteen, joten lainsäädännöllä ei voida määritellä tietoturvan tasoa sopimuspalokunnissa. Esimerkiksi kulunvalvonta on tietoturvaa, mutta lailla ei voida vaatia, millainen täytyy olla kulunvalvonnan taso päästääkseen paloasemalle. Kuitenkin vapaaehtoisuuden pohjalta voidaan määritellä tietoturvantasoa sekä tietosuojaa. Sitä kautta tulee mahdolliseksi käyttää erilaisia lainsäädännön keinoja myös sopimuspalokuntatoiminnassa.

Suomessa sopimuspalokunnat toimivat itsenäisesti omien sääntöjen mukaan. Ne ovat itse suunnitelleet säännöt yhdistystoiminnan perusteella. Näin ollen jokaisella sopimuspalokunnalla on Suomessa omat säännöt, miten toimitaan. Kuitenkin sopimuspalokuntien toiminta perustuu alueellisten pelastuslaitosten kanssa tekemiin sammutussopimuksiin. Näin ollen pelastuslaitosten antamien ohjeiden mukaan voidaan vaatia tiettyä tietoturvan tasoa. Kuitenkaan kaikki tietoturvaan liittyvät asiat eivät suoraan määräydy sopimuspalokuntien omista säännöistä, vaan alueen pelastuslaitos voi vaikuttaa tai jopa määrätä tietyn tason, jota on noudatettava. Yhdistykset tietyn väliajoin tarkastelevat omia sääntöjään, ja tällöin sinne voisi lisätä kirjauksen salassapitoasioista.

Jokainen yhdistys toimii omien sääntöjen mukaan, varsinkin nykyään kannattaa suositella, että huomioidaan tietoturva ja tietosuojataso. Se, että miten näitä huomioidaan, on yhdistysten välinen oma asia.

Kun on sitouduttu noudattamaan tiettyä tietoturvan tasoa, tulee silloin sellaiset lainsäädännöt huomioida, jotka koskettavat sopimuspalokuntatoimintaa.

Oulu-Koillismaan pelastuslaitoksen alueella sopimuspalokunnilla ei ole yhtenäistä käytäntöä tietoturvasta. Tämä tarkoittaa sitä, että ei ole samanlaista koulutusta asiaan, vaikka Oulun kaupunki on tehnyt kaikkia henkilöitä koskevat tietoturvaohjeet, joihin henkilöstön tulisi tutustua ja saada koulutusta. Harjoitusohjelmia laadittaessa ja harjoituksia pidettäessä toimivat sopimuspalokunnat omien toiveiden mukaisesti. Pääpaino harjoituksissa on laadittu sen mukaan, mitkä ovat mahdolliset tehtävät erilaisissa onnettomuustilanteissa, jolloin tietoturva–asiat ovat jääneet vähemmälle huomiolle. Lisäksi tietoturvaan vaikuttaa se, millä paikkakunnalla palokunta sijaitsee ja miten siellä on tietoturvaan varauduttu ja suhtauduttu. Tällä on merkitystä, kun pelastuslaitos toimii pääsääntöisesti vuokralaisena eri kunnissa. Tällöin täytyy huomioida se, mikä on vuokranantajan halu tietoturvaan ja miten sopimuspalokunnat yhdessä pelastuslaitoksen kanssa ovat valmiita huomioimaan tietoturvaa.

5 SOPIMUSPALOKUNTIEN MERKITYS SUOMESSA JA OULU - KOILLISMAAN PELASTUSLIIKELAITOKSELLA

Suomessa on 22 alueellista pelastuslaitosta. Jokainen pelastuslaitos on alueellaan kehittänyt omien tarpeidensa mukaisesti paloasemaverkoston. Näiltä paloasemilta hoidetaan onnettomuuksien sattuessa sammutus- ja pelastustehtävät. Asemien henkilöstö muodostuu päätoimisista viranhaltijoista, joita on (112 asemaa) ympärivuorokautisesti tai sopimushenkilöstöstä (709 asemaa). (Koivunen 2015, 6.)

Suomessa on, pois lukien Ahvenanmaa, 491 yhdistyspalokuntaa (vpk), 18 työpaikkasopimuspalokuntaa ja 200 sivutoimista, jotka ovat tehneet henkilökohtaisen sopimuksen pelastuslaitoksen kanssa. Näissä palokunnissa toimii 13400 hälytyskelpoista henkilöä, jotka ovat saaneet samanlaisen koulutuksen ympäri Suomen ja joilla on samanlaiset kelpoisuusvaatimukset sekä osallistumista harjoituksiin sekä hälytyksiin ympäri valtakunnan. (Koivunen 2015, 8.)

Pelastuslaitosten toimintamenot, jossa on huomioitu päätoiminen henkilöstö sekä sivutoiminen henkilöstö, on noin 400 miljoonaa euroa. Näistä menoista on arvioitu, että sopimuspalokuntien osuus on noin 72,8 miljoonaa euroa vuodessa eli vajaan viidenneksen verran. Yhden sopimushenkilöstön kustannukset ovat keskimäärin 5433 euroa vuodessa. (Koivunen 2015, 6.)

Pelastustoiminnan kannalta sopimuspalokuntien osuus on varsin merkittävä. Jos asia katsotaan pinta-alan mukaan, sopimuspalokunnat huolehtivat pelastustehtävistä noin 90 % maamme alueen pinta-alasta. Tällä alueella asuu Suomen väestöstä noin 46 % asukkaista. (Koivunen 2015, 3.)

5.1 Vpk – sopimuspalokunta

Vpk on yhdistysmuotoinen, vapaaehtoisella periaatteella toimiva sopimuspalokunta, joka on tehnyt alueen pelastuslaitoksen sammutus- ja pelastustehtävien sekä muiden erikseen sovittujen palveluiden tuottamisesta. Esimerkiksi ensivastetoimintaa, harjoittaa noin 200 sopimuspalokuntaa. (Koivunen 2015, 10.)

Yleensä sopimuspalokuntatoiminnassa on hälytysosaston lisäksi muitakin osastoja. Esimerkkinä mainittakoon nuoriso-osasto, veteraaniosasto ja naisosasto. Keskimäärin yhden sopimuspalokunnan vuosibudjetti on 30000 euroa. (Koivunen 2015, 10.)

Tavanomainen sopimuspalokunta on tehnyt sammutussopimuksen alueen pelastuslaitoksen kanssa, jolla on keskimäärin seitsemänkymmentä jäsentä. Jäsenistä noin kaksikymmentä kuuluu hälytysosastoon. Sopimuspalokunnassa on myös muita osastoja oman sopimuspalokunnan toiminnan mukaan. Pääsääntöisesti niitä ovat nuoriso-osasto, jossa on keskimäärin viisitoista jäsentä ja naisosasto, jossa on keskimäärin kymmenen jäsentä. Lisäksi on muita osastoja, esimerkiksi veteraaniosasto. Näissä muissa osastoissa on noin kaksikymmentäviisi jäsentä. Lisäksi sopimuspalokunnalla on päällikkö ja puheenjohtaja sekä hallitus ja jäsenistön kokous. Tällaisen sopimuspalokunnan käytössä olevaan kalustoon kuuluu sammutusauto, säiliöauto, miehistöauto, peräkärry ja vene sekä traileri (Koivunen 2015, 11).

5.2 Henkilökohtainen sopimuspalokunta

Henkilöt ovat tehneet työsopimuksen suoraan pelastuslaitoksen kanssa, muuten toimivat samalla tavalla kuin sopimuspalokunnat. Usein henkilöstöllä on oma palomiesyhdistys, ja toiminnassa on samoin mukana nuoriso-, nais- ja veteraanitoimintaa. Osallistuminen hälytystehtäviin ja harjoituksiin perustuu sopimuksiin kuten sopimuspalokunnilla. (Koivunen 2015, 12.)

Tavanomaisella henkilökohtaisella sopimuspalokunnalla on keskimäärin kaksikymmentä hälytyskelpoista jäsentä. He ovat perustaneet palomiesyhdistyksen, jolla on puheenjohtaja ja hallitus sekä jäsenistön kokous. Heillä on kalustona käytettävissä suunnilleen samanlaiset kuin vpk:lla eli sammutusauto, säiliöauto, miehistöauto, peräkärry ja vene sekä traileri. (Koivunen 2015, 13.)

5.3 Sopimuspalokunta toiminta Oulu-Koillismaan pelastusliikelaitoksella

Oulu-Koillismaan pelastusliikelaitos toimii Oulun läänin alueella. Alue on pinta-alaltaan suuri, ja välimatkat varsinkin Itäisellä toimialueella ovat pitkiä. Tämä luo oman haas-

teensa sopimuspalokuntatoimintaan, varsinkin kun pelastuslaitoksen alueella on vakinainen palokunta ympärivuorokautisessa toiminnassa ainoastaan Kuusamossa, Oulussa, Kempeleellä ja Haukiputaalla (Oulu-Koillismaan pelastusliikelaitos 2012.)

Oulu-Koillismaan pelastustoimen alueella toimii seitsemäntoista sammutussopimuksen tehnyttä sopimuspalokuntaa yhdistysmuotoisena tai sivutoimisina henkilöstöinä palomiesyhdistysten kautta. Yhteensä toiminnassa vuonna 2014 on ollut 381 henkilöä. (Määttä 2015.)

Alueen sopimuspalokunnat ovat vapaamuotoista varallaolossa sellaisilla paikkakunnilla, joissa ei ole vakinaista henkilökuntaa ympäri vuorokauden. Näillä paikkakunnilla, joissa on vakinainen henkilöstö ympärivuorokauden, on sopimuspalokunnilla sammutussopimuksessa määritelty vpk-valmius, missä ajassa täytyy tietty määrä henkilöstä osallistua hälytystehtäviin. Esimerkiksi Oulussa on valmius sovittu sammutussopimuksessa 1 + 4 viidessätoista minuutissa ja Kuusamossa 0 + 2 kymmenessä minuutissa. Hälytykset tulevat virven, matkapuhelimen tai piipparin eli hakulaitteen kautta.

Vuoden 2014 aikana alueen sopimuspalokunnilla oli 2028 tehtävää. Näistä tehtävistä kaksi eniten ollutta olivat ensivastetehtävät (446 kpl) ja liikenneonnettomuudet (354 kpl) eli noin 40 % kaikista tehtävistä. (Määttä 2015.)

Nämä kaksi onnettomuustyyppiä ovat tietosuojan kannalta merkittäviä, väheksymättä yhtään muita tehtäviä. Ensivastetehtävissä saadaan erilaista tietoa asiakkaista, se voi olla myös tietoa, joka ei kuulu muille kuin tehtävässä mukana olleille. Tämä tarkoittaa esimerkiksi sitä, että potilaslomakkeista huolehditaan niin, että niitä ei näe muut kuin tehtävään osallistuneet. Samoin joskus voi tulla eteen purkutilaisuus tehtävästä, johon osallistuu ainoastaan tehtävään osallistuneet henkilöt. Näin voidaan estää turhan tiedon levittäminen palolaitoksen sisällä.

Liikenneonnettomuudet ovat varsinkin sosiaalisen median tai eri lehtien kautta kiinnostavia onnettomuustyyppejä. Usein lehdissä näkee ilmoituksen, että lähetä kuva, maksamme palkkion, tai tiedätkö jotain asiasta, kerro vihje. Tällaisiin asioihin ei pidä mennä mukaan. Osalla sopimuspalokunnissa on näihin asioihin nollatoleranssi, ettei mitään kuvia tai tietoja saa kertoa sosiaalisessa mediassa tai lehdissä eteenpäin. Täytyy muistaa, että tiedottaminen kuuluu pelastustoiminnan johtajalle, joka on pelastusviranomainen.

6 OULUN KAUPUNGIN TIETOTURVAPOLITIIKKA

Nykyisin varmasti suurimmassa osassa erilaisissa työpaikoissa (valtio, kunnat, yritykset) on tietoturva-asiat otettu vakavasti. On laadittu erilaisia tietoturvaohjeita tavoitteena saada työpaikoilla yhteiset käytänteet tietoturva-asioihin.

Tietoturvapolitiikan määrittelyyn ei ole olemassa yksiselitteistä määrittelyä, vaan jokainen toimija määrittelee itse tietoturvapolitiikan. Tietoturva-asiakirjat voivat olla julkisia ja näkyvillä esimerkiksi nettisivuilla tai työpaikan ilmoitustaululla. Näin voi nähdä, miten on suhtauduttu tietoturvaan, millaisia näkemyksiä ja tavoitteita on asetettu. Kun johto sitoutuu noudattamaan tietoturvapolitiikkaa, koskee se myös kaikkia työntekijöitä ja velvoittaa myös noudattamaan tietoturvapolitiikkaa. (Järvinen 2002, 113.)

Myös Oulun kaupunki on laatinut itselleen tietoturvapoliittisen ohjeen, se koskee kaikkia kaupungin työntekijöitä riippumatta siitä onko kyseessä virkasuhde tai työsopimussuhde. (Oulun kaupungin tietoturvapolitiikka 2013, 3.)

Laadittaessa erilaisia ohjeita ja visioita, tulee niihin määritellä tavoitteet. Ensimmäisenä asiana tietoturvaan liittyen tulee miettiä ja arvioida riskit ja uhkakuvat. On tiedossa, että tietoturvaan liittyvät asiat ovat jatkuvasti erilaisten uhkien kohteena.

Organisaatiolle laaditaan ja vahvistetaan tietoturvaohjeet käytännön tilanteisiin. Tämän tarkoituksena on ohjata henkilöstön tietoturvatoimintaa. Tiedon turvallista käsittelyä kannattaa korostaa henkilöstölle. Tietoturvapolitiikka kannattaa hyväksyä riittävän korkealla tasolla organisaatiossa, jolloin tarkoituksena on, ettei uusimisen tarvetta ilmenisi kovin usein. (Andreasson ja Koivisto 2013, 34.)

Oulun kaupunki on jakanut omat tavoitteet kuuteen eri osa-alueeseen

1. Tunnistetaan tietoturvaan liittyvät uhkatekijät. Tavoitteena on tunnistaa kaupungin kannalta tärkeimmät ja merkittävimmät uhkatekijät sekä riskit, jotka vaikuttavat tietoturvaan. (Oulun kaupungin tietoturvapolitiikka 2013, 6.)

2. Saadaan pidettyä erilaisten tietojärjestelmien, tietoverkkojen ja tietojenkäsittelyyn liittyvien toiminta jatkuvasti toiminnassa ilman keskeyttämistä, havaitaan tarvittaessa ja myös estetään tietojen luvaton käyttö ja pyritään suojaamaan elintärkeät toiminnot mahdollisimman lyhyellä toipumisajalla kaikissa häiriötilanteissa, jos vain tilanne sitä vaatii (Oulun kaupungin tietoturvapolitiikka 2013, 6).

3. Tietoturva-asioihin annetaan koulutusta koko henkilöstölle. Tunnistetaan, millaiset ovat tietoturva ohjeet ja noudatetaan annettuja ohjeita. Jokaiselle työntekijälle annetaan säännöllisesti koulutusta, jonka tavoitteena on ylläpitää luottamusta kaupungin tarjoamiin palveluihin ihmisten ja sidosryhmien välillä, että tietoturva, tietosuoja ja yksityisyydensuoja toteutuisi. (Oulun kaupungin tietoturvapolitiikka 2013, 6)

4. Huomioidaan, että tietoturva toteutuu toimintaketjujen kautta kokonaisuudessaan. Toimintaketjuun kuuluvat palvelujentoimittajat, yhteistyökumppanit ja alihankintaketjut. Heidän on sitouduttava noudattamaan kaupungin tietoturvapolitiikkaa, ja mikäli huomataan sopimuksessa poikkeamia, on raportoitava asiasta eteenpäin. Samoin on huolehdittava, että tietojen tietoturvasta huolehditaan asianmukaisella tavalla. (Oulun kaupungin tietoturvapolitiikka 2013, 6.)

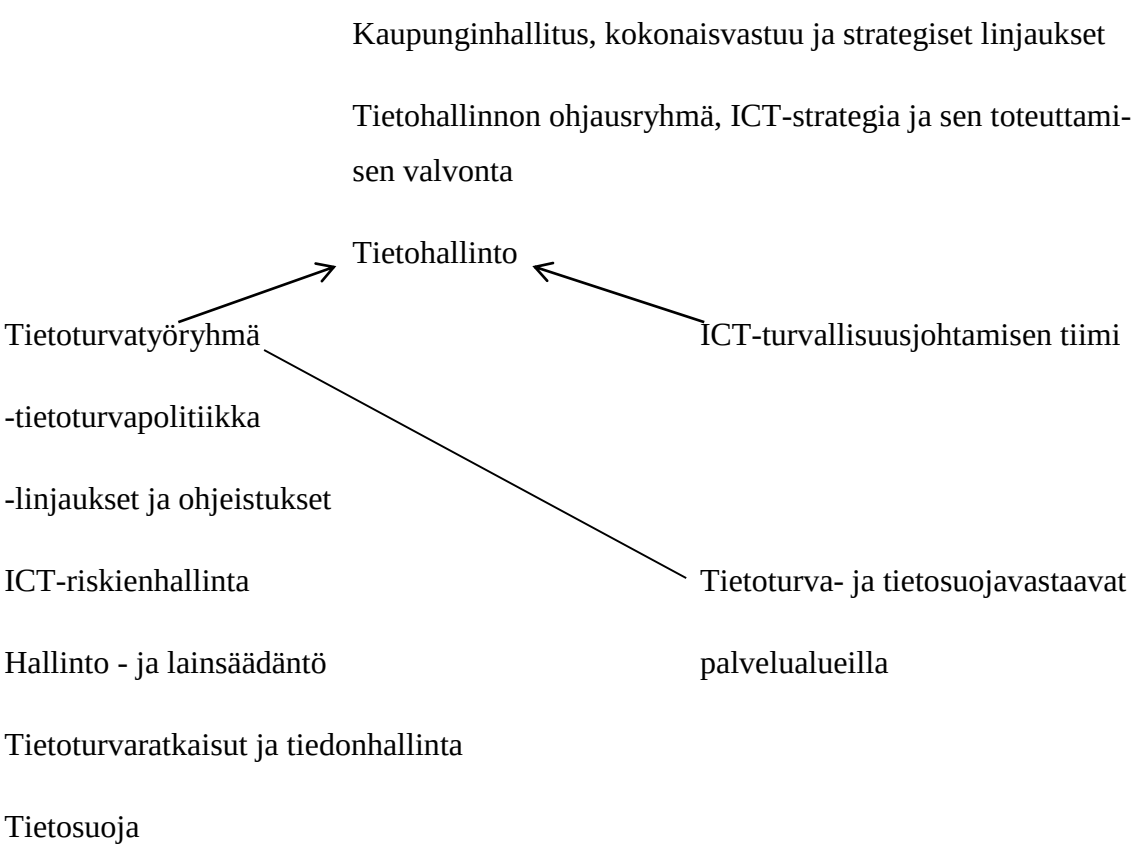
5. Tietoturvallisten toimintamallien erilainen kehittäminen antaa uusia mahdollisuuksia päivittäiseen toimintaan palvelutuotannon tukemiseen, kun voidaan hyödyntää uudenlaista teknologiaa. Tällöin voidaan erilaisissa toimintaympäristössä luotettavien ratkaisujen avulla saada mahdollisimman tehokas ja tietoturvallinen työskentely riippumatta ajasta, paikasta tai työvälineistä. (Oulun kaupungin tietoturvapolitiikka 2013, 7.)

6. Vahti-tietoturvaohjeistus ja kansainväliset tietoturvastandardit ovat lähtökohtana tietoturvatyöhön. Näin saataisiin tiedot suojattua parhaiten normaalioloissa tai häiriötilanteissa hallinnollisin tai teknisin toimenpitein. (Oulun kaupungin tietoturvapolitiikka 2013, 7.)

Perustana tietoturvatyön toteutumiselle on kaupunginhallituksen hyväksymä tietoturvapolitiikka ja määritellyt ohjeistukset. Niistä löytyvät toimintamallit ja vastuut tietoturvapolitiikkaan. (Oulun kaupungin tietoturvapolitiikka 2013, 8.)

Oulu–Koillismaan pelastuslaitos tuottaa omalla alueellaan pelastustoimen palvelut ja isäntäkuntana on Oulun kaupunki. Näin ollen sopimuspalokuntalaiset ja sivutoiminen henkilöstö ovat tehneet sopimukset pelastuslaitoksen kanssa osallistumisesta pelastustoimintaan ja harjoituksiin. Tätä kautta olisi hyvä myös tutustua isäntäkunnan tietoturvaohjeisiin, että tiedetään, mitä asioita ajatellaan.

Oulun kaupunki on jakanut vastuut tietoturvatyöhön:



(Oulun kaupungin tietoturvapolitiikka 2013, 8).

7 KYSELYT JA HAASTATTELUT

Webropol-kysely ja haastattelut suoritettiin vuoden 2015 kevään ja kesän aikana. Webropol-kysely antaa mahdollisuuden kyselyn mukaan vastata väittämiin kyllä tai ei. Tämän lisäksi jokainen kyselyyn osallistuva sai kertoa näkemyksiä olennaisiin asioihin vaihtoehtokysymyksiin. Haastatteluissa tehtiin tarkennettuja kysymyksiä tietoturvasta ja tietotosuojasta. Kysely lähetettiin jokaiselle alueen sopimuspalokunnalle, sopimuspalokunnan päällikölle tai yksikönjohtajalle, sivutoimisille palomiesyhdistyksille sekä henkilöstölle, jotka hyväksyvät tai laativat harjoitusohjelmat. Alueella toimii seitsemäntoista sopimuspalokuntaa tai sivutoimista palomiesyhdistystä. Webropol-kysely löytyy liitteestä 1.

Mielestäni yhdelle henkilölle tai palokunnalle lähetetyt kysymykset ovat perusteltuja, koska sopimuspalokunnan päällikkö tai harjoitusohjelmien laatija ja hyväksyjä edustaa omaa palokuntaansa ja sitä, mitä harjoituksissa harjoitellaan ja milloin. Harjoitusohjelman hyväksyjä tai kouluttaja toimii pääsääntöisesti viranhaltijana pelastuslaitoksella. Yleensä jäsenistö ei osallistu harjoitusohjelmien tekoon, vaan sen tekevät edellä mainitut henkilöt.

Sellaisista palokunnista, joista ei tullut kohtuuajassa vastauksia tai edes avattu lähetettyä kyselyä, sain esille uusia henkilöitä, jotka voisivat vastata kyselyyn. Siitä huolimatta vastausten saaminen kesti mielestäni liian kauan. Tein asian selvittämiseksi muutamia lisäasioita, esimerkiksi haastattelin henkilöitä tapaamisen merkeissä, puhelimitse ja sähköpostiviestien välityksellä. Haastattelurunko, jota käytin, löytyy liitteestä 2.

Hälytysosastoissa oli mukana 381henkilöä vuonna 2014. Vastauksia Webropol-kyselyyn tuli sopimuspalokunnista ja palomiesyhdistyksiltä koskien 221 henkilöltä eli vastaukset edustivat 58 % alueen henkilöstöstä. Vastauksia tuli kymmeneltä henkilöltä. Alunperin kysymykset lähetettiin seitsemälletoista henkilölle. Myöhemmässä vaiheessa kysymyksiä lähetettiin vielä neljälle henkilölle täydentämään kyselyä.

Webropol-kyselyn ja haastattelujen yhteenveto

Vaikka osa vastaajista toimii pelastuslaitoksella viranhaltijoina, ovat he myös mukana sopimuspalokuntatoiminnassa. Palokuntatoiminnasta vastaajilla on pitkä kokemus. Puolet vastaajista on ollut mukana toiminnassa yli 20 vuotta ja loputkin kuudesta vuodesta viiteentoista vuotta. Näin he pystyvät hyvin arvioimaan koulutukseen liittyviä asioita.

Heillä on tietoa siitä, millaista koulutusta on järjestetty, ja he pystyivät arvioimaan myös sitä, millaista koulutusta voisi tulevaisuudessa järjestää.

Eri tietoturva osa-alueista saadaan näkemyksiä, millainen näkemys ja kokemus vastaajilla on tietoturva ja tietosuoja – asioihin. Hallinnollinen tietoturva on tietoturvan kivijalka. Hallinnollinen tietoturvallisuus on organisaation johdon hyväksymää tietoturvapolitiikkaa. Tässä työssä voidaan käyttää hyvänä esimerkkinä Oulun kaupungin laatimaa tietoturvaohjeistusta, joka koskee kaikkia työntekijöitä.

Tietoaineistoturvallisuuden merkitystä korostettiin. Tietoaineisto koostuu esimerkiksi asiakirjoista ja erilaisista tiedostoista. Asiakirjoista löytyy asiakkaiden tietoja. Ne on tarkoitettu ainoastaan heidän tietoonsa, jotka ovat osallisena tehtävään. Tämä näkyy siinä, että hälytystehtävistä noin neljäsosa on ensivastetehtäviä, jolloin joudutaan käsittelemään potilastietoja. Prontoon sopimuspalokuntalaiset eivät pääse tekemään onnettomuusselosteita, vaan asian hoitaa eri paloasemilla pelastusviranomainen. Kaikki tieto ei ole aina verkossa, vaan samoja tietoja voi löytyä kirjallisena.

Henkilöstöturvallisuuden osalta uusi turvallisuusselvityslaki astui voimaan vuoden 2015 alussa. Tämä laki antaa mahdollisuuden tehdä turvallisuusselvityksen henkilöstä, joka on tulossa mukaan toimintaan. Tällä pyritään parantamaan henkilöstöturvallisuutta. Turvallisuusselvityksen mahdollisuutta pidetään hyvänä asiana, ja vastaajista kaikki olivat sitä mieltä, että se on tarpeellinen tai sitä voisi harkita, vaikka tähän asti sen käyttö on ollut vähäistä. Vastaajista ainoastaan kahdessa tapauksessa on tehty turvallisuusselvitys ja nämä on tehty ennen uuden turvallisuusselvityslain voimaantuloa. Kuitenkin kaikki vastaajista pitivät turvallisuusselvitystä tarpeellisena tai sitä harkittavana. Nyt uuden lain myötä tähän on mahdollisuus, että turvallisuusselvitys tehdään, joten aika näyttää, tuleeko tähän jatkossa muutosta.

Henkilöturvallisuuteen kuuluu myös tietoturvaan liittyvä koulutus. Koulutuksen merkitystä korostettiin ja sitä pidetään tärkeänä. Puolet vastaajista kertoi, että tietoturva- ja tietosuoja-asioita on käyty läpi. Käytännössä näin on tehty perehdyttämisvaiheessa. Koulutusta tarvitaan aiheeseen enemmän. Perehdyttämisvaihe on osa henkilöstöturvallisuuteen liittyvää tietoturvaa. Siinä käydään läpi, millaista sopimuspalokuntatoiminta on. Perehdyttämisvaiheessa nousi esille salassapitosopimus. Vastaajista kahdeksan vaati kirjallista salassapitosopimusta, joka tehdään perehdyttämisvaiheessa tai kun liitytään mukaan toi-

mintaan. Salassapitosopimuksessa jäsen omalla allekirjoituksella lupaa pitää omana tietona toiminnassa saamansa tiedot. Salassapitosopimuksella tarkoitetaan vaitiolovelvollisuutta.

Uskon, että tämä opinnäytetyö aiheena saa koulutuksista vastaavat henkilöt miettimään ja käymään läpi tietoturva ja tietosuoja-asioita. Vastaajat pitivät tärkeänä, että asia on noussut esille. Selvisi, että koulutukselle on tarvetta, että ei riitä se, mitä käydään läpi asioista perehdyttämisvaiheessa.

Käyttöturvallisuuden osalta selvisi, että sopimuspalokuntalaiset eivät pääse pelastuslaitoksen sisäiseen verkkoon, eikä heille ole myönnetty Pronton käyttöoikeuksia. Näitä oikeuksia on ainoastaan alueen pelastusviranomaisilla. Tällainen asia on perusteltua, koska tieto siellä kuuluu viranomaistoimintaan.

Tietoliikenneturvallisuudella on yhteyttä käyttöturvallisuuteen. Kun sopimuspalokuntalaiset eivät pääse sisäiseen verkkoon, silloin voidaan pitää turvallisena sitä asiaa, että he eivät pääse tietoihin, joita verkossa on, esimerkiksi viranomaisten asiakirjat. Päätoimisen henkilöstön käyttöä tietoliikenneturvallisuuden osalta huolehtii Oulun kaupungin tietohallinto, jota kautta on hoidettu virustorjunta, huolehtii, että salasanat vaihtuvat tietyin väliajoin, ja antaa käyttöoikeudet tietoverkkoihin.

Fyysiseen turvallisuuteen kuuluu kulunvalvonta. Asemapaikoilla, joissa toimii vakinainen palokunta yhdessä sopimuspalokuntien kanssa, on käytössä sähköiset lukot, jotka toimivat kulunvalvontalätkällä. Alueella Oulun sopimuspalokunnalla on omat tilat, muut sopimuspalokunnat käyttävät tiloja ja kalustoa yhdessä pelastuslaitoksen kanssa. Tarvittaessa toiminnasta poisjääviltä kerätään kulkuluvat pois. Tällöin pystytään varmistamaan, etteivät ulkopuoliset enää pääse tiloihin.

Vierailujen yhteyteen ei ole järjestetty vierailuja varten omia sääntöjä, vaan silloin toimitaan henkilöstön antamien ohjeiden mukaan. Huolehditaan siitä, että vierailijat eivät liiku asemilla yksin. Jotain tehtäviä asemilla tekevät myös talon ulkopuoliset henkilöt, jotka on perehdytetty siihen, miten kohteessa työskennellään ja toimitaan. Lisäksi tällaiset työt on sovittu etukäteen, hyvänä esimerkkinä on siivous.

Myös mahdollisten onnettomuuksien tai häiriötekijöiden varalta on suunnitelmia. Tietoja varmuuskopioidaan ja käytetään pilvipalveluita. Lisäksi tietoja säilytetään paperiversioina.

Oulun kaupunki tehnyt omat tietoturvaohjeet työntekijöilleen, ja säännösten mukaan ne koskettavat kaikkia kaupungin palveluksessa olevia työntekijöitä, niin virkamiehiä kuin työsopimussuhteessa olevia henkilöitä. Näin ollen ohjeet koskettavat myös sopimuspalokuntalaisia toimiessaan palokuntatehtävissä ja sivutoimista henkilöstöä myös, koska he ovat tehneet suoraan työsopimuksen alueen pelastuslaitoksen kautta. Kyselyssä tuli esille se, että tietoturva- ja tietosuoja-asioita on käyty läpi perehdyttämisvaiheessa. Samoin siinä vaiheessa on käyty läpi kaupungin tietoturvaohjeistusta, näin totesi puolet vastaajista. Mielestäni olisi hyvä kaikkien tietää, että kaupunki on laatinut tällaiset ohjeet.

Tietosuojan kannalta varallaolo on tärkeä asia, koska silloin voidaan saada monenlaista tietoa, joka koskee ainoastaan toimintaan osallistuville. Tarkoituksena on, ettei saatua tietoa levitetä ulkopuolisille henkilöille. Vapaamuotoisen varallaolon aikana ei olla jatkuvasti fyysisesti paloasemalla, vaan liikutaan ja ollaan ihmisten kanssa tekemisissä eri paikoissa.

Vastausten perusteella tärkein tekijä, jolla turvataan tietosuoja varallaolon aikana varsinkin julkisilla paikoilla, on, että virve pidetään äänettömänä ja virven kaiutin on pois päältä, eli niin sanottua äänetöntä virven käyttöä. Samoin tuli esille, että kaikki viestintävälineet ovat mukana. Kotioloissa voivat muut perheenjäsenet saada tietoa, joten heille täytyy kertoa tietosuojasta, mitä se tarkoittaa. Kuitenkin mahdollisesti saatu tieto varallaolon aikana perustuu salassapitovelvollisuuteen pelastuslain 86 §:n mukaisesti.

Nykyisin sosiaalinen media voi haastaa ihmisiä. Sinne voi laittaa ja jakaa sellaista tietoa, jolla on ”markkina-arvoa”, mutta joka kuuluu salassapitovelvollisuuden piiriin.

Kannattaa miettiä, ennen kuin on lähettämässä mitään tietoa sosiaaliseen mediaan, onko se sallittua ja hyväksyttävää. Viestityksen, joka on julkista, poistaminen on vaikeaa. Haastattelussa kävi ilmi, että tällaisista asioista seuraa sanktioita, mikäli näin tekee, että jakaa kuvia, videoita tai kirjoittaa omista tehtävistä pelastustoiminnan aikana. Mikäli haluaa sosiaalisessa mediassa jakaa tietoa, kannattaa esimerkiksi perustaa omat facebook-sivut ja siellä kertoa yleisellä tasolla omasta toiminnasta, esimerkiksi päivä paloasemallatapahtumista tai harjoituskauden avauksista, jolloin otetaan mukaan uusia henkilöitä mukaan toimintaan.

Varallaoloa tekevät näyttävän tietävän tietoturvasta ja tietosuojasta hyvin. Tämä näkyi siinä, kun he saivat vastata, miten tietosuojasta on huolehdittu varallaolon aikana. Kuitenkin kyselyssä tuli ilmi, että koulutus on jäänyt vähäiseksi ja asiaan pitäisi panostaa enemmän. Varallaoloa tekevät pitempään toiminnassa mukana olevat tai esimiesasemassa olevat henkilöt. Samoin nämä henkilöt toimivat kouluttajina sopimuspalokunnissa. Heillä on sitä tietoa, mutta tietoa pitäisi jalkauttaa harjoituksiin.

8 POHDINTA

Opinnäytetyön aiheena tietoturva ja tietosuoja ovat laaja. Helposti voi käydä niin, että työ laajenee liian suureksi. Kun yrittää varoa tätä, että näin ei käy, on mahdollisuus, että työ jää liian suppeaksi. Olisi heti alussa tärkeää rajata työn aiheeseen liittyvä tutkimusongelma, mitä halutaan selvittää.

Aiheeseen liittyvää materiaalia löytyy suhteellisen hyvin. Varsinkin netistä löytyy kaikenlaista tietoa, ja helposti voi käydä, että luottaa niihin liikaa. Kuitenkin kirjallinen lähdeaineisto on työn perusta ja nettilähteet voivat täydentää työtä.

Kyselytutkimuksessa joutui miettimään, kenelle ja kuinka paljon kysymyksiä esitettiin. Jos jokaiselle toimintaan osallistuvalle, henkilöitä noin 400 olisi tehty, se olisi ollut ainakin minulle suuri urakka. Täytyy muistaa, että opinnäytetyö on 15 opintopistettä. Kuitenkin jokaisella sopimuspalokunnalla on päällikkö, harjoitusohjelmien laatija tai kouluttaja. Heidän vastuullaan on se, mitä harjoituksissa käydään läpi. He huolehtivat millainen tietoturvataso on sopimuspalokunnissa. He edustavat omaa palokuntaansa. Siksi tuntui mielekkäämmältä tehdä heille kysely ja haastattelut.

Opinnäytetyö on myös oppimistilanne. Aiheen mukaan pääsee tai saa tutustua erilaisiin asioihin ja tilanteisiin. Tässä työssä olen saanut huomattavan paljon lisätietoa alun lähtötilanteeseen. Aiheen laajuus, mitä tietoturva ja tietosuoja ovat, yllätti jonkin verran työn edetessä. Samoin kirjallisen työn osuus ensimmäistä kertaa tässä laajuudessa oli haastavaa. Kyselytutkimusta tehdessä kannattaa huolellisesti valmistaa ennakolta kysymykset varsinkin Webropol-kysymysten osalta, ettei jälkeenpäin tule mieleen asioita, mikäli jokin asia, johon haluaa vastauksen, jää pois kyselystä. Toki on mahdollista jälkeenpäin saada vastauksia esimerkiksi haastatteluilla.

Tietoturvaan liittyvät asiat ja siihen liittyvät erilaiset uhat ovat lähes päivittäin esillä eri medioissa. Näin ollen tietoturva-asiat ovat esillä ja ihmisten tietoisuudessa. Tieto liikkuu nykyisin nopeasti esimerkiksi verkossa ja tietoturvaan on oltava valmis reagoimaan. Täytyy pystyä tunnistamaan riskit. Tietoturvassa on useita riskitekijöitä. Helposti kuvitellaan, tietokone tai verkossa tapahtuva liikenne tai toiminta suurin uhkatekijä tietoturvalle ja tietosuojalle. Todellisuudessa ihminen on se suurin uhka tietoturva-asioihin.

Tietoturva-asiat ovat pelastustoimessa suhteellisen uusi asia, samoin koko yhteiskunnassa. Ei tarvitse mennä useita vuosikymmeniä taaksepäin, kun tällaisesta asiasta ei ollut

vielä mitään tietoa. Tekniikan ja tiedon lisääntyessä ovat pikkuhiljaa nämä asiat nousseet esille. Ihmisistä on saatavilla paljon tietoa eri rekistereistä, voi välillä kysyä jopa sitä, mihin kaikkeen niitä tarvitaan.

Helposti uusien asioiden esille tuominen tai ajatus siitä, että tietoturva on tärkeää myös pelastustoimessa, varsinkin jos kyse on harrastustoiminnasta, voi nostaa esille muutosvastarintaa. Mielletään asiat helposti esimerkiksi, että kumpi on tärkeämpää, tietää hyvät käytännöt tietoturvasta ja tietosuojasta vai osata tehdä perusselvitys.

Tietoturvasta huolehtiminen on asennekysymys. Ihmisten asenteisiin voidaan vaikuttaa kouluttamalla henkilöstöä ja perustelemalla myös, miksi tietoturva on tärkeä asia. Tietoturvasta huolehtiminen täytyy lähteä liikkeelle johdosta käsin näyttämällä omaa esimerkkiä.

Palokunnissa on tiedostettu, että tietoturvasta huolehtiminen on tärkeä asia. Se, että asia on tiedostettu, on hyvä, mutta se ei vielä mielestäni riitä. Se, että vaaditaan vaitioloa tiedoista, joita saadaan erilaisista tehtävistä, ei riitä vielä tietoturva-asioiden hyvään hoitamiseen. Kuitenkin tietoturva käsitteenä on erittäin laaja.

Vastuu alueen sopimuspalokuntien tietoturvakoulutuksesta kuuluu niille, jotka laativat harjoitusohjelman. Vaikka tietoturva-asiat on tiedostettu, ei niitä ole juurikaan käyty läpi harjoituksissa. Tämä näkyi siinä, kun kerrottiin, että tietoturva-asiat ovat jääneet vähemmälle huomiolle tai asiaa pitäisi enemmän nostaa esille ja muistuttaa, kuinka tärkeästä asiasta on kysymys. Koettiin myös, että kun kyseessä harrastustoiminta, asia kuuluu enemmän viranhaltijoille, ja ettei asia varsinaisesti kosketa sopimuspalokuntia. Tietoturva-aiheen esille nostaminen opinnäytetyön aiheena sai positiivista palautetta.

Tietoa tietoturva-asioihin on olemassa paljon ja sitä kannattaa hyödyntää. Sopimuspalokunnat voisivat esimerkiksi kerran harjoituskauden aikana käydä läpi harjoituksissa tietoturva-asioita ja korostaa samalla niiden merkitystä jäsenilleen. Vaikka aihe käsitteenä on laaja, siitä pystyy poimimaan olennaisimmat asiat sopimuspalokunta toimintaan.

LÄHTEET

Andreasson, A. ja Koivisto, J. 2013. *Tietoturvaa toteuttamassa.* AS Pakett. Tallinna.

Tietosuojavaltuutetun toimisto. 2015. *Lait*. www-dokumentti. http://www.tietosuoja.fi/fi/index/lait.html. 27.10.2015

Hakala, M., Vainio, M. ja Vuorinen, O. 2006. *Tietoturvallisuuden käsikirja.* WS Bookwell. Porvoo

Henkilötietolaki 523/1999.

Helopuro, S., Perttula, J. ja Ristola, JP. 2004. *Sähköisen viestinnän tietosuoja.* Gummerus Kirjapaino Oy. Jyväskylä

Hirsjärvi, S., Remes, P. ja Sajavaara, P. 2005. *Tutki ja kirjoita.* 11. painos. Gummerus Kirjapaino Oy. Jyväskylä

Hirsjärvi, S. ja Hurme, H. 2008. *Tutkimushaastattelu, Teemahaastattelun teoria ja käytäntö.* Yliopistopaino. Helsinki

Innanen, A. ja Saarimäki, J. 2009. *Internet–oikeus.* Edita Prima Oy. Helsinki

Järvinen, P. 2012. *Arjen tietoturva.* Saarijärven Offset Oy. Saarijärvi

Järvinen, P. 2002. *Tietoturva & yksityisyys.* WS Bookwell. Porvoo

Koivunen, P. 2015. *Pelastustoimi ja sopimuspalokunnat Suomessa - Suomen sopimuspalokuntien liiton julkaisuja, sarja c:4/2015.* toinen painos. Eura Print Oy

Koivunen, P. 2014. *Sopimuspalokunnat Suomessa.* Eura Print Oy

Kokkala, R. 2010. *Tietoturvariskien hallinta pelastustoimessa.* Diplomityö. Tampereen teknillinen yliopisto. Tampere.

Korhonen, R. 2003. *Perusrekisterit ja tietosuoja.* Edita Prima Oy. Helsinki

Laki viranomaisten toiminnasta julkisuudesta 621/1999.

Laki yksityisyydensuojasta työelämässä 759/2004.

Määttä, V. 2015. Sähköpostiviesti 26.3.2015.

Oulun kaupungin tietohallinto. 2013. *Oulun kaupungin tietoturvapolitiikka.* Oulun konttori, Painatuskeskus. Oulu

Oulu-Koillismaan pelastusliikelaitos. 2012. *Palvelutasopäätös 2013 - 2016.* www-dokumentti. http://pelastuslaitos.ouka.fi/tiedotteet/Palvelutasopaatos%202013%20-%202016.pdf. 20.3.2015

Pelastuslaki 379/2011.

Pesonen, P. 2012. *Yritysviestinnän säännöt.* Bookwell Oy. Jyväskylä

Rikoslaki 39/1889, virkarikoksista 604/2002.

Rikoslaki 39/1889, tieto- ja viestintärikoksista 578/1995.

Turvallisuusselvityslaki 726/2014.

Valtiovarainministeriö. 2006. *Tietoturvallisuuden arviointi valtion hallinnossa 8/2006.* Edita Prima Oy. Helsinki

Valtiovarainministeriö. 2008. *Tärkein tekijä on ihminen–henkilöstöturvallisuus osana tietoturvallisuutta.* Edita Prima Oy. Helsinki

Liite 1

1. Toimitko pelastuslaitoksella? *

Viranhaltijana

Sivutoimisena

Sopimuspalokuntalaisena

2. Oletko? *

Mies

Nainen

3. Mikä on ikäsi? *

18-25

26-35

36-45

46-55

yli 55

4. Oletko toiminut sopimuspalokuntalaisena tai pelastuslaitoksen palveluksessa? *

1-5 vuotta

6-10 vuotta

11-15 vuotta

16-20 vuotta

yli 20 vuotta

5. Toimitko palokunnassa tai pelastuslaitoksella? *

Sammutusmiehenä

Yksikönjohtajana

Sopimuspalokunnan päällikkönä

Miehistössä

Alipäällystössä

Päällystössä

6. Oletko tutustunut Oulun kaupungin tietoturva ohjeisiin? *

En

Kyllä

7. Oletteko harjoituksissa käyneet läpi tietoturva-asioita? *

Kyllä

Ei

8. Mikäli ette ole käyneet tietoturva/suoja-asioita läpi, niin voisiko harjoituksissa niitä käydä läpi? *

Kyllä

Ei

9. Pidätkö tietoturvaan/tietosuojaan liittyviä asioita tärkeänä? *

Kyllä

En

10. Mitä mielestäsi tietosuoja tarkoittaa pelastustoimessa? *

11. Pääsettekö laitoksen sisäiseen verkkoon? *

Kyllä

En

12. Onko käytössä Pronto tunnuksia? *

Kyllä

Ei

13. Miten kulunvalvonta on teidän asemalla järjestetty? *

14. Suoritatteko varallaoloa/päivystystä? *

Kyllä

Ei

15. Millä teidät hälytetään hälytystehtävään? *

Virve

Matkapuhelin

Piippari

Jokin muu

16. Miten huolehditte tietosuojasta varallaolon aikana? *

17. Kuka rekrytoi lisää henkilöitä palokuntaanne? *

18. Miten rekrytoitte lisää henkilöitä? *

19. Teettekö kuntotestit uusille jäsenille? *

Kyllä

Ei

20. Vaaditteko uusilta jäseniltä salassapitosopimusta kirjallisesti? *

Kyllä

Ei

Riittää suullisesti

21. Teettekö turvallisuusselvitystä uusille jäsenille? *

Kyllä

Ei

22. Olisiko turvallisuusselvitys tarpeellinen? *

Kyllä

Ei

Voisi harkita

23. Kuka kouluttaa asemallanne nuoriso-osastoa? *

24. Koetko tietoturvaan/suojaan liittyvät asiat tärkeänä? *

Kyllä

En

25. Vapaa sanaa / kommentointia halutessasi

Liite 2

1. Onko tietosuojaa ja tietoturvaa koskevat ohjeet saatavilla henkilöstöllä? Miten?

2. Onko tietosuojaa ja tietoturvaa koskevista ohjeista koulutettu ja tiedotettu riittävästi? Mitä asialle voisi tehdä?

3. Edellyttääkö pääsy tietojärjestelmiin henkilökohtaista käyttäjätunnusta ja salasanaa?

4. Miten on tehty toimenpiteet murto, palo ja kiinteistövahinkojen ehkäisemiseksi? Onko olemassa kaikenvaralta järjestelyitä?

5. Onko tietojärjestelmiä varten olemassa varajärjestelmät ja suunnitelmat? Millaiset?

6. Seurataanko ja valvotaanko henkilötietojen käytön ja käsittelyn lainmukaisuutta säännöllisesti? Miten?

7. Onko jatkuva viruksentorjunta järjestetty?

8. Onko tietoturva huomioitu, hankittaessa uusia tietovälineitä ja sovelluksia? Miten?

9. Onko tietojenkäsittelyn jatkuvuus huolehdittu huolto ja ylläpitosopimuksilla?

10. Onko järjestetty riittävä tietoturvakoulutus henkilöstölle? Miten on järjestetty, jos on riittävä?

11. Oletko varmistanut, että vaitiolo ja salassapitosopimukset ovat osa työsopimusta? Miten olet?

12. Varmistatko, että salasanat vaihdetaan riittävän usein?

13. Varmistatko, että salasanoja ei vaihdeta suusanallisesti?

14. Oletko varmistanut, että asiakirjojen säilyttämisestä on annettu riittävät ohjeet ja määräykset?

15. Oletko varmistanut, ettei kukaan ulkopuolinen pääse sisäiseen verkkoon? Miten?

16. Oletko varmistanut, ettei sisäisessä verkossa sivulliset pääse henkilötietoihin?

17. Oletko varmistanut, että on olemassa kulunvalvontajärjestelmä, joka estää luvattoman henkilön liikkumisen tiloissa ja että valvontajärjestelmä on koko ajan toiminnassa? Tämä siis, jos on käytössä.
18. Oletko varmistanut, että kulkuoikeudet loppuvat palvelusuhteen päätyttyä?

19. Oletko huolehtinut, että ulkopuolisen henkilöstön (esim. siivoojat) sisäänpääsyoikeudet tiloihin on määritelty heidän suorittamiensa tehtäviensä mukaan?

20. Oletko varmistanut, että vierailijoita varten on vierailijasäännöt, joita noudatetaan käytännössä?

21. Tarvitaanko kulkulupa, vai tullaanko ”kyläilemään” ihan perinteiseen tapaan?

22. Oletko varmistanut, että lyhyidenkin poissaolojen aikaan on annettu ohjeet huoneiden ja päätteiden sulkemisesta? Miten toimit?

23. Oletko varmistanut, että tilat joissa järjestelmään sisäänpääsyn mahdollistavat päätteet ovat ja tilat, joissa säilytetään henkilötietoja sisältäviä asiakirjoja, on valvottu myös työajan jälkeen?